International Journal of Advanced Multidisciplinary Research and Educational Development
Volume 2, Issue 2 | March – April 2026 | www.ijamred.com
ISSN: **3107-6513**

Digital Forensic Analysis of USB Device Using System Artifacts

R. Mageshwari[1], R. Karan[2]
[1,2]*Department of Computer Science, Rathinam College of Arts and Science (Autonomous), Coimbatore, Tamil Nadu, India.*
[2]*Corresponding Author:mahimagesh74@gmail.com*

Abstract - *The rapid increase in cyber threats has made data security a critical concern for individuals and organizations. USB devices, which are widely used for data transfer, can also be misused for unauthorized data access and data theft. These activities can be detected through system artifacts such as Windows Registry and system logs. However, manual analysis of these artifacts is inefficient and time-consuming.This paper presents an automated digital forensic analysis system designed to analyze USB device usage using Windows system artifacts. The system focuses on extracting information from registry entries related to USB devices and applies device-based, time-based, and user-based analysis techniques to identify suspicious behaviour. Threshold-based conditions are used to classify activities into different severity levels.The proposed system generates a structured forensic report that improves investigation efficiency and reduces manual effort. The results demonstrate that the system provides accurate detection of USB usage patterns and enhances overall cybersecurity monitoring.*

Keywords *- USB Forensics, Digital Forensics, Registry Analysis, USB Device Analysis, Cybersecurity, System Artifacts, Log Analysis*

1. Introduction

In the modern digital era, the widespread use of portable storage devices such as USB drives has significantly increased the risk of data security threats. USB devices are commonly used for transferring and storing data due to their convenience and portability. However, they can also be misused for unauthorized data access, data theft, and the introduction of malicious software into computer systems.

Operating systems such as Windows maintain various system artifacts that record device usage activities. These artifacts include Windows Registry entries and system logs, which store important details about connected USB devices. Information such as device name, vendor ID, product ID, and connection timestamps can be extracted from these artifacts and used for forensic investigation.

Digital forensic analysis plays a crucial role in identifying and investigating such activities. By analyzing system artifacts, investigators can track USB device usage history and detect suspicious behavior. However, manual analysis of registry data and logs is time-consuming and requires technical expertise. It becomes difficult to handle large volumes of data and identify meaningful patterns without automated tools.

His creates a need for an efficient system that can automatically collect, process, and analyze USB-related data. In this project, an automated digital forensic analysis system is proposed to examine USB device usage using Windows system artifacts. The system applies various analysis techniques to identify patterns and detect suspicious activities.

The proposed approach improves investigation efficiency, reduces manual effort, and enhances the accuracy of detecting unauthorized USB usage. It provides a reliable solution for digital forensic investigations and helps strengthen overall cybersecurity.

2.Existing System

In the existing system, the analysis of USB device usage is carried out manually by examining Windows Registry entries and system logs. Investigators need to navigate through registry paths such as USBSTOR to identify connected devices and extract relevant information.

This approach has several limitations. Firstly, it is time-consuming, especially when dealing with large amounts of data. Secondly, it requires technical knowledge to understand and interpret registry data accurately. Additionally, identifying patterns such as repeated device connections or suspicious usage is difficult without automated support.

ISSN: 3107-6513

The existing system also lacks a structured reporting mechanism. Investigators must manually collect and organize the data, which increases the chances of human error. Furthermore, there is no automatic detection or alert system to identify unauthorized USB usage.

Due to these limitations, the existing approach is inefficient and not suitable for modern digital forensic investigations.

3. Proposed System

In the existing system, the analysis of USB device usage is carried out manually by examining Windows Registry entries and system logs. Investigators need to navigate through registry paths such as USBSTOR to identify connected devices and extract relevant information.

This approach has several limitations. Firstly, it is time-consuming, especially when dealing with large amounts of data. Secondly, it requires technical knowledge to understand and interpret registry data accurately. Additionally, identifying patterns such as repeated device connections or suspicious usage is difficult without automated support.

The existing system also lacks a structured reporting mechanism. Investigators must manually collect and organize the data, which increases the chances of human error. Furthermore, there is no automatic detection or alert system to identify unauthorized USB usage.

Due to these limitations, the existing approach is inefficient and not suitable for modern digital forensic investigations.

4.Literature Survey

In recent years, digital forensic analysis has gained significant importance in identifying and investigating cyber-related activities. Several research works have focused on analyzing system artifacts such as Windows Registry and log files to track user activities and connected devices.

Traditional approaches mainlyon manual analysis using tools like Registry Editor and Event Viewer. These methods provide detailed information about system activities, but they are time-consuming and require technical expertise. Identifying patterns such as repeated USB connections or suspicious device usage becomes difficult without automated support.

Some advanced forensic tools such as Autopsy and FTK Imager are used for analyzing digital evidence. These tools provide better visualization and structured analysis, but they may be complex for beginners and require proper training to use effectively.

Recent studies emphasize the use of automated techniques and scripting languages like Python to simplify forensic analysis. Automation helps in extracting relevant data from system artifacts and identifying patterns more efficiently.

The proposed system builds upon these approaches by providing a simple and automated solution for analyzing USB device usage using Windows Registry artifacts. It focuses on improving efficiency, reducing manual effort, and enhancing the accuracy of digital forensic investigations.

5.Methodology

The proposed system follows a systematic methodology to analyze USB device usage using Windows system artifacts. The entire process is divided into multiple stages, including data collection, data processing, analysis, and report generation. Each stage plays an important role in identifying suspicious USB activities accurately.

5.1 Data Collection

The first stage involves collecting USB-related data from the Windows operating system. The system extracts information from Windows Registry entries, specifically from paths related to USB devices such as USBSTOR. These entries contain important details about connected devices.

5.2 Data Processing

After collecting the data, the next step is processing. The raw registry data contains unnecessary and unstructured information. The system filters and extracts only the required details such as device name, vendor ID, product ID, and connection timestamps. This ensures that the data is clean and ready for analysis.

ISSN: 3107-6513

5.3 Analysis Techniques

Once the data is processed, the system performs detailed analysis using different techniques to identify suspicious behavior:

- Device-Based Analysis: Identifies frequently connected USB devices.
- Time-Based Analysis: Detects repeated connections within short time intervals.
- User-Based Analysis: Tracks USB usage across different users.
- Threshold-Based Detection: Classifies activities based on predefined limits to identify abnormal usage.

Figure 1: System Architecture

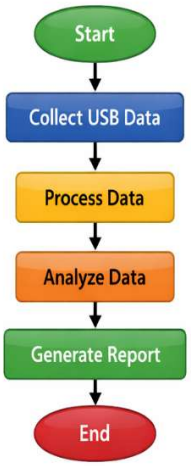

Figure 2: Forensic Analysis Flowchart

5.4 Report Generation

After completing the analysis, the system generates a structured forensic report. The report includes details such as list of connected USB devices, usage patterns, and detected suspicious activities. This helps investigators easily understand and analyze the results.

6. Results and Discussion

The proposed system was tested using Windows registry data containing multiple USB device connection records. The system successfully extracted relevant information such as device name, vendor ID, product ID, and connection timestamps from system artifacts.

The results show that the system effectively identifies USB device usage patterns using different analysis techniques. Frequently connected devices and repeated connections within short time intervals were successfully detected as part of the analysis.

The discussion indicates that the automated approach significantly improves the efficiency of forensic investigation compared to manual methods. Manual analysis requires more time and technical expertise, whereas the proposed system provides faster and more accurate results.

The system also reduces human errors by automating data extraction and analysis. Overall, the proposed system enhances digital forensic investigation by providing reliable detection of USB device activity and generating structured reports.

7. Conclusion

This project presented an automated digital forensic analysis system for examining USB device usage using Windows system artifacts. The system focuses on extracting and analyzing data from Windows Registry entries to identify connected USB devices and their usage patterns.

The proposed system successfully automates the process of data collection, processing, and analysis. By eliminating manual investigation, it reduces the time and effort required for forensic analysis. The system also improves accuracy by minimizing human errors and providing consistent results.

The implementation of analysis techniques such as device-based, time-based, and user-based analysis helps in identifying suspicious USB activities effectively. Threshold-based detection

ISSN: **3107-6513**

further enhances the system's ability to classify abnormal behavior.

The generated forensic report provides clear and structured information about USB device usage, making it easier for investigators to understand and take necessary actions. Overall, the system serves as an efficient and reliable solution for USB device forensic analysis and supports cybersecurity investigations.

8. Future Scope

The proposed system can be further enhanced by implementing real-time monitoring of USB device activities. This will help in detecting unauthorized device usage instantly and improve system security. An alert mechanism can also be added to notify users or administrators when suspicious USB activity is detected.

Future improvements can include the development of a graphical user interface (GUI) to make the system more user-friendly and easier to operate. Data visualization techniques such as charts and graphs can be integrated to represent USB usage patterns clearly.

The system can also be extended to support analysis of other system artifacts and external storage devices, making it a more comprehensive digital forensic tool. Integration with advanced security systems and intrusion detection systems can further enhance its effectiveness in cybersecurity environments.

9. References

1. Microsoft Corporation, *Windows Registry Documentation*, Available: https://learn.microsoft.com/en-us/windows/win32/sysinfo/registry
2. Nelson, B., Phillips, A., & Steuart, C., *Guide to Computer Forensics and Investigations*, Cengage Learning, 2018.
3. Casey, E., *Digital Evidence and Computer Crime*, Academic Press, 2011.
4. NIST, *Guide to Integrating Forensic Techniques into Incident Response (SP 800-86)*, 2006.
5. Stallings, W., *Network Security Essentials*, Pearson Education, 2016.
6. Garfinkel, S., "Digital Forensics Research: The Next 10 Years," *Digital Investigation Journal*, 2010.
7. Bejtlich, R., *The Practice of Network Security Monitoring*, No Starch Press, 2013.